Khudiakova Elena Alekseevna
Student
Ural Federal University
Russia, Ekaterinburg
Academic supervisor: Kovaleva Alexandra Georgievna

NFC TECHNOLOGY AND ITS INFORMATION SECURITY

Abstract. *NFC data transfer begins when compatible devices are combined. Data transmitted between two smartphones via NFC is not encrypted, therefore a modern problem of personal data security becomes rationale, as we live in the world of the Internet, gadgets and various information threats. This paper presents the results of the analysis of data hiding technologies that may ensure the safe transfer of information, as well as protect information from theft by intruders.*

Keywords: *NFC technology, personal data protection, mobile technologies, information security, data hiding.*

Худякова Елена Алексеевна
Студент
Уральский федеральный университет
Россия, г. Екатеринбург
Научный руководитель: Ковалёва Александра Георгиевна

ТЕХНОЛОГИЯ NFC С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *Передача данных NFC начинается при объединении совместимых устройств. Данные, передаваемые между двумя смартфонами через NFC, не шифруются, поэтому возникает современная проблема безопасности персональных данных, ведь мы живем в мире Интернета,*

гаджетов и различных информационных угроз. В данной статье представлены результаты анализа технологий сокрытия данных, которые могут обеспечить безопасную передачу информации, а также защитить информацию от кражи злоумышленников.

Ключевые слова: *Технология NFC, защита персональных данных, мобильные технологии, информационная безопасность, сокрытие данных.*

INTRODUCTION

Innovative technologies are introduced into the lives of ordinary people. It is very important to ensure the safety of each person. Every day is full of worries and troubles. In the daily rush, you need to find things very quickly. Do you know what's inside a woman's bag? It's a real nightmare. You need a credit card everywhere – in the store, pharmacy, transport. When you need to react quickly, NFC is an indispensable technology. The subject of this paper is NFC technology and its information security. The purpose of this paper is to give an overview of the NFC technology in various spheres of life, the reasons for information leaks and methods of protection from scammers.

NFC TECHNOLOGY AND ITS INFORMATION SECURITY

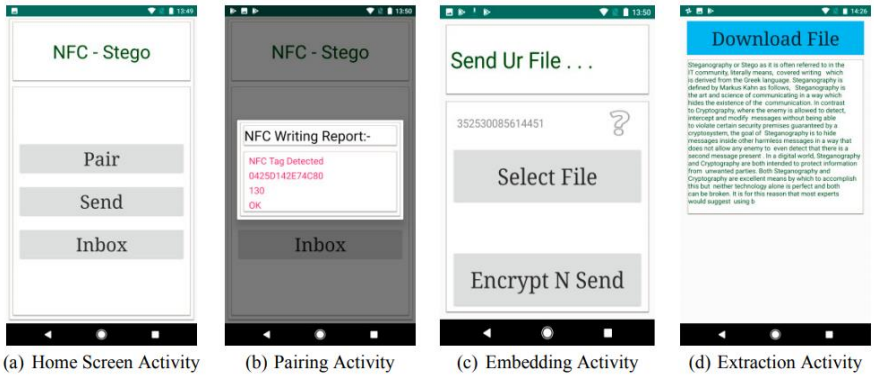
Many applications have become available by the integration of near field communication (NFC) into smartphones with the progressive development of smartphones. This technique solves one of the most difficult problems of hiding open data-recovery of deleted files (cover-files), which can help in extracting the payload from the stego file (Stego-analysis).

NFC is characterized as an agreement on short-distance correspondence, which, in fact, is proposed to be used on a cell phone [3]. It is powered by the in-novation of radio frequency identification (RFID), a contactless structure that uses radio waves of recurrence (RF) to exchange or confirm information over a short distance. It is

important to remember that there are two sides to each NFC session: the initiator and the target [4].

Data hiding is one of the popular methods by which private data is protected by hiding it in the other data [1]. The main goal is to hide personal data in the cover media (media; media that contains personal data, which can be text, images, videos, or audio files [1], while only end users are aware of the hidden data.

The system consists of three main methods, which are the mating technique, the embedding technique, and finally the extraction technique. The design of these methods is implemented in Android smartphones with NFC support. To use the system, both users should have a special application (Figure).



(a) Home Screen Activity (b) Pairing Activity (c) Embedding Activity (d) Extraction Activity

Figure 1. NFC-Stego Application

There are three main operations in the system.

1) The mating process. The sender receives the recipient's international mobile equipment ID (IMEI) of the android smartphone that was recorded on the NFC tag by shaking the tag with the receiving phone;

2) The embedding process, which is completely based on the sender. The sender selects the secret data to be encrypted and embedded. They are encrypted using the recipient's IMEI as the key leading to the encrypted data. Finally, this encrypted data will be embedded on the server based on its IMEI;

3) The extraction process. The receiver using your IMEI associated with the phone system should be checked for any new secret data. If any new data related to its

IMEI is detected, the system automatically retrieves it from the server, decrypts it using the IMEI, and then displays it to the recipient.

The system is more secure than any data concealment system, because the embedding process is based on digital cover media, meaning that an attacker from a distance of 10 cm will not be able to intercept data, since it is necessary to reach a distance of 4 cm. In addition, a data encryption algorithm was performed before the embedding process to improve system security.

The invisibility of this system is determined by the fact that no one can detect the difference between the cover and the original signal [3]. This is important for methods that use a digital cover that has data embedded in it, but in the NFC-Stego system, the data was embedded in the hard cover. For example, the system can be embedded in a book cover, bus card, keychain, and more.

Thus, the considered method solves one of the most difficult tasks of hiding open data-recovery of deleted files (cover-files), which can help in extracting the payload from the stego file (Stego-analysis). The main advantage is the ability to embed into any hard surface, which provides security and data hiding. The same security system is considered, but with the addition of virtual reality (VR) technology. Virtual Reality (VR) is the world created by technical means, transmitted to a person through his perceptions: vision, hearing, touch, and others. Virtual reality simulates both exposure and reactions. Computer synthesis of virtual reality properties and reactions is performed in real time to create a convincing set of reality sensations.

The design of the system for sending and receiving secret messages is based on an NFC-compatible android smartphone, VR images and international mobile equipment identification (IMEI), which is a unique number for each mobile phone, allowing each client to be recognized by their device [2]. The system consists of three main methods: the mating technique, the embedding technique, and finally the extraction technique. These methods are discussed above. Accordingly, a step is added to encrypt the information into the image, which is transmitted to the recipient and then decrypted (Figure).

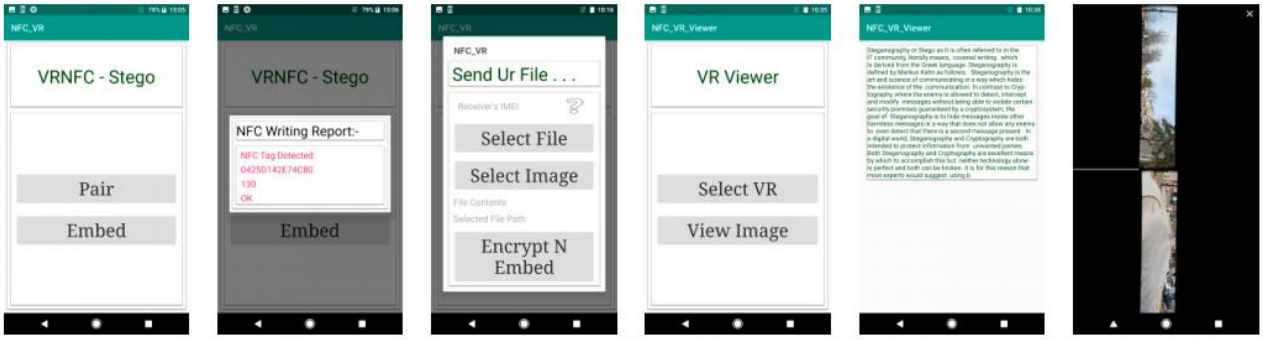


Figure 2. VRNFC-Stego Application

It is important for the information security of the technology that VR images do not arouse suspicion, since they can be used in various areas in everyday life. In addition, there are no stegoanalysis methods applied to VR images.

The method solves the security problem of hiding data, since no one receives the embedded message inserted in the VR image, except the receiver, which performs the pairing process at the beginning of the system, where, like any other receivers, can view the VR image only through the application. VRNFC-Stego allows you to hide high-capacity data in cover media (VR images) due to the high resolution. In addition, the use of VR technology in data hiding is new, which makes VR images not suspicious and not under the control of stegoanalystics.

CONCLUSION

Thus, this article demonstrates two important technologies that may be presented in everyday life. Data hiding in NFC-enabled smartphones includes two areas: with virtual reality technology and classic data hiding. This paper reveals current problems that are changing at the speed of light.

REFERENCES

1. Abdelmgeid Ali, Al-Hussien Seddik Saad, Ahmed Hamdy Ismael. Data Hiding Technique Based on NFC-Enabled Smartphones. – 2020. – Text: electronic. –

URL: https://www.sciencedirect.com/science/article/pii/S1877050920312527 (Reference date 18.12.2020).

2. Abdelmgeid Ali, Al-Hussien Seddik Saad, Ahmed Hamdy Ismael. VRNFC-Stego: Data Hiding Technique based on VR Images and NFC-Enabled Smartphones. – 2020. – Text: electronic. – URL: https://www.sciencedirect.com/science/article/pii/S1877050920311455 (Reference date 20.12.2020).

3. Luigi Sportiello. Internet of Smart Cards: A pocket attacks scenario. – 2019. – Text: electronic. – URL: https://www.sciencedirect.com/science/article/pii/S1874548219300642 (Reference date 17.12.2020).

4. Utsav Jambusaria, Neerja Katwala, Dharmeshkumar Mistry D.J.Sanghvi. Secure Smartphone Unlocking using NFC. – 2015. – Text: electronic. – URL: https://www.sciencedirect.com/science/article/pii/S1877050915003178 (Reference date 21.12.2020).